carahsoft

VIDIZMO.AI

ThŜ C2dzNJ tλffI-NJă 2Ŧ a2ŘŜNJy tdzōfλǑ {I-ŦŜűè

! DdzλŘŜ Ŧ2NJ [I·ǿ 9yŦ2NJǑŜYˇŜyű [ŜI·ŘŜNJă

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through and a wide range of contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with VIDIZMO, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/VIDIZMOresources

Join Events & Webinars:
carah.io/events

Discover Technology Solutions:
carah.io/VIDIZMOsolutions

Learn About Procurement:
carah.io/VIDIZMOcontracts

Connect With Our Team:
LawEnforcement@carahsoft.com
833-221-5529

VIDIZMO.AI

Whitepaper

The Four Pillars of Modern Public Safety: A Guide for Law Enforcement Leaders

This whitepaper examines the four core operational workflows that define modern law enforcement: real-time surveillance, digital evidence management, investigation, and public records disclosure. It explores where traditional approaches fall short, what leading agencies are doing differently, and how purpose-built technology supports a more secure, efficient, and accountable approach across each pillar.

Executive Summary

Law enforcement agencies face an unprecedented convergence of operational pressures. Body-worn cameras are standard equipment. Digital evidence is present in roughly 90 percent of criminal cases. Public records laws demand faster, more rigorous disclosure than most agencies were built to deliver. And investigators are expected to close cases faster with the same or fewer resources.

These pressures are interconnected. The footage captured by a patrol officer's body-worn camera becomes evidence in an investigation, is reviewed by a detective developing leads, and is eventually processed for public disclosure. Each workflow is governed by different standards, handled by different personnel, and supported by different systems, yet each depends on the workflow before it.

Many agencies continue to manage these functions as separate operational domains. Surveillance technology is managed by IT. Evidence custody belongs to the evidence unit. Investigations are handled by detectives. Records requests are processed by the records office. This siloed structure was adequate when evidence volumes were manageable and public records requests were infrequent. It is no longer sufficient.

This whitepaper examines the four pillars of modern public safety (surveillance, digital evidence management, investigation, and public records disclosure) and presents a framework for understanding how they connect, where traditional approaches break down, and how purpose-built technology enables a more secure, efficient, and accountable operational model.

Table of Contents

The State of Modern Public Safety Operations

Digital evidence has become foundational to how law enforcement agencies establish facts, demonstrate accountability, and fulfill their public obligations. Video recordings, audio files, digital documents, and surveillance data now serve as primary sources of truth in investigations, legal proceedings, and public disclosures. Research from the Department of Justice indicates that digital evidence is present in approximately 90 percent of criminal cases, underscoring how thoroughly the evidentiary landscape has shifted.

At the same time, the volume of digital evidence that agencies generate and manage has grown at a pace that most operational infrastructures were not designed to absorb. The average officer equipped with a body-worn camera generates between 7 and 13 gigabytes of video data per shift. When multiplied across a department and a full year of operations, the storage, processing, and review burden becomes substantial. The Jefferson County, Colorado District Attorney's Office processed more than 67,700 videos totaling 41,000 hours of footage in a single year. That figure had nearly doubled from 36,000 videos and 24,000 hours just three years earlier. A routine vehicular homicide case in that jurisdiction now generates 362 photographs (up from 79 in 2017) and up to 90 hours of body-worn camera and dash cam footage (up from zero in 2017).

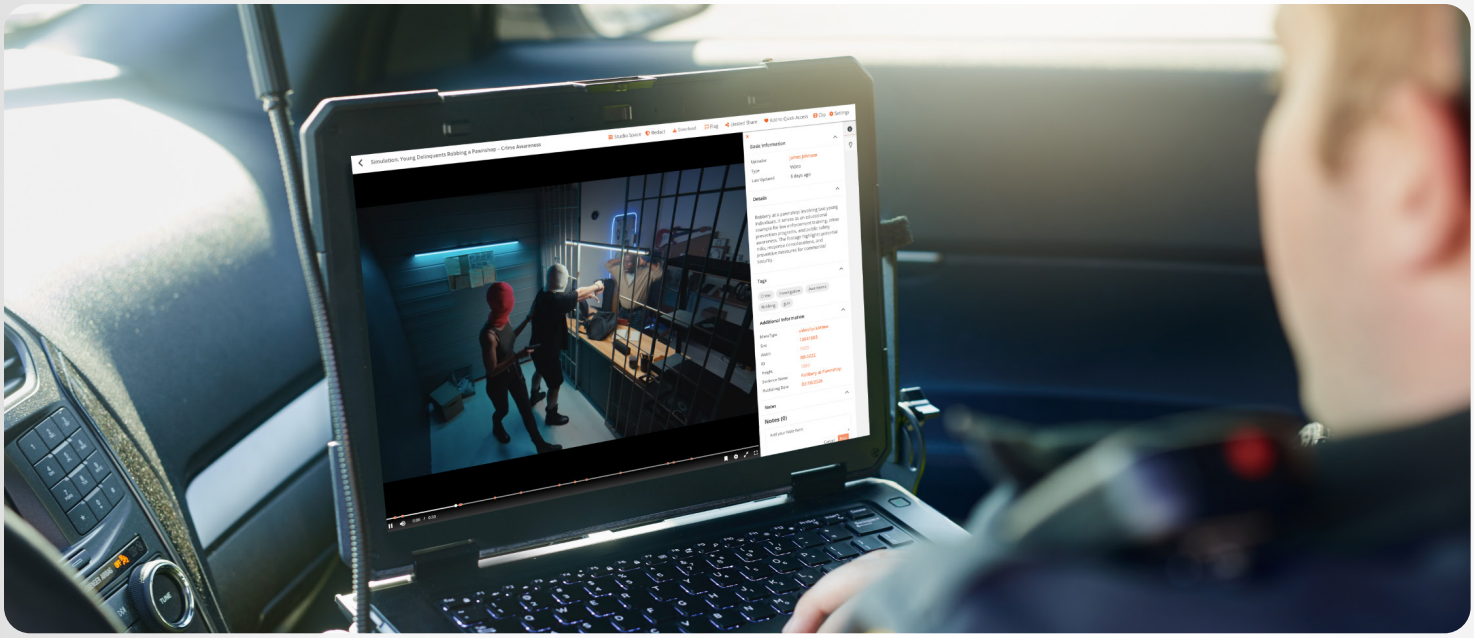
This volume challenge intersects with intensifying legal and regulatory obligations. Courts expect evidence to be produced completely, authentically, and on time. The principles established in Brady v. Maryland require prosecutors to disclose all material evidence that could be favorable to the defense, a standard that is increasingly difficult to meet when evidence is scattered across multiple systems and formats. Public records laws at the state level impose strict timelines on the disclosure of government records, including body-worn camera footage.

In Missouri, this obligation is codified in Chapter 610 of the Revised Statutes, known as the Sunshine Law. The statute establishes a presumption that all records of public governmental bodies are open to the public unless a specific provision of law allows or requires closure. Section 610.023.3 requires that each request for access to public records be responded to as soon as possible, but no later than the end of the third business day following receipt. Courts may impose civil fines of up to $1,000 for knowing violations and up to $5,000 for purposeful violations, along with costs and attorney fees. In 2025 alone, the Missouri Attorney General's office received 337 Sunshine Law complaints, nearly one for every day of the year, with a third remaining unresolved.

Despite these pressures, many agencies still rely on workflows and systems designed for an earlier era. Evidence is managed in silos. Review processes are manual and labor-intensive. Sharing mechanisms are informal and difficult to audit. Redaction is performed by hand, one file at a time. These approaches are no longer sustainable at current and projected evidence volumes.

Meeting the demands of modern public safety requires rethinking how the four core operational pillars work, both individually and as a connected whole. The following section defines each pillar and establishes the framework for understanding how they relate to one another.

The Evidence Crisis: Why Current Systems Are Failing



The volume of digital evidence agencies generate has outpaced the operational infrastructure designed to manage it. The consequences are felt at every stage, from collection to courtroom to public disclosure.

90% of criminal cases now involve digital evidence (Department of Justice)

67,700 videos processed by Jefferson County DA in a single year

337 Sunshine Law complaints filed in Missouri in 2025 alone

A routine vehicular homicide case in Jefferson County, Colorado now generates 362 photographs and up to 90 hours of body-worn camera and dash cam footage, figures that were effectively zero in 2017. Courts expect complete, authenticated evidence produced on schedule. Brady v. Maryland requires disclosure of all material evidence favorable to the defense. Missouri's Sunshine Law mandates response to public records requests within three business days, with civil penalties of up to $5,000 for purposeful violations.

Many agencies still manage these obligations with siloed systems, manual review processes, and informal sharing mechanisms. These approaches cannot scale to meet current volumes, let alone projected growth.

The Four Pillars of Modern Public Safety

Modern law enforcement operations depend on four interconnected workflows. Together, they define the full arc of a public safety event, from initial detection through final public disclosure.

Surveillance

How agencies monitor environments in real time to detect threats, deter crime, and generate a contemporaneous record. Includes fixed infrastructure, body-worn cameras, and vehicle-mounted systems.

Digital Evidence Management

How agencies ingest, store, secure, and share digital evidence from collection through disposition, including chain of custody, retention policies, and legal hold enforcement.

Investigation

How detectives and analysts locate, review, and interpret evidence to develop leads, build timelines, and construct cases across large, multi-format evidence sets.

Redaction & Disclosure

How agencies fulfill public records obligations, identifying and redacting protected information, preparing releasable materials, and documenting disclosure decisions for legal defensibility.

These pillars are not parallel functions. They are sequential stages of a single workflow. What surveillance captures shapes what evidence management must handle. The quality of evidence governance determines how effectively investigation proceeds. The completeness of investigation defines what disclosure must address.

Where Traditional Operations Break Down

Traditional approaches rely on disconnected systems, manual workflows, and organizational structures not designed for current scale. Because the pillars are connected, failures compound across the entire chain.

Surveillance: Reactive Rather Than Real-Time

Most law enforcement camera infrastructure was deployed with recording as the primary objective, and footage is reviewed after an incident is reported, not while it is developing. Studies show that operator attention degrades significantly after approximately 20

minutes of continuous video monitoring. For agencies monitoring dozens of camera feeds, the odds of catching a specific event in real time are low.

Weapons near schools, unauthorized vehicles in restricted areas, suspicious activity at critical infrastructure: these scenarios cannot wait for after-the-fact review. The International Association of Chiefs of Police has recognized that surveillance technology must be accompanied by the capability to process and act on data in real time if the investment in infrastructure is to deliver its full operational value. Agencies that deploy cameras without an analytical layer are capturing evidence of what already happened, rather than enabling intervention in what is still developing.

> *Core Gap: Cameras record. No one is truly watching. The response comes after the event, not during it.*

Evidence Management: Fragmented and Exposed Real-Time

Digital evidence arrives from body-worn cameras, dash cams, interview rooms, 911 systems, drones, surveillance infrastructure, and case documents. In most agencies, each source feeds a different system under different access policies. This fragmentation undermines chain of custody, the requirement that every transfer, access, and modification be documented from collection onward. The Department of Justice's guidance on digital evidence handling emphasizes that inconsistencies in chain of custody documentation can undermine the authenticity and admissibility of evidence in court. When evidence is copied to a thumb drive or shared via email without a formal access log, the chain weakens. These are among the most common grounds on which digital evidence is challenged.

Fragmented management also delays investigations and increases Brady violation risk. When evidence must be located across multiple systems before it can be reviewed, the time to prepare a case for prosecution grows beyond what discovery deadlines allow.

> *Core Gap: Evidence scattered across systems creates chain of custody exposure, delays investigations, and increases legal risk.*

Investigation: The Review Bottleneck

A case that once involved a handful of witness statements may now include 90 hours of footage, hundreds of photographs, and thousands of pages of documents. The evidence exists, but finding the moments that matter is where investigative capacity is consumed. Detectives describe spending the majority of their time reviewing footage and preparing summaries rather than developing leads or interviewing witnesses. The National Academy of Sciences has identified this growing administrative burden as a structural challenge to investigative effectiveness.

The operational consequence is case backlog. When investigators spend hours reviewing footage to locate minutes of relevant material, other cases are not being worked. When a critical piece of evidence is not located because a search of physical media did not surface it, a lead is missed. This is not a personnel problem; it is a process and technology problem that has grown alongside evidence volumes without a corresponding increase in review capacity.

Core Gap: Investigators drown in evidence volume. The bottleneck is not personnel; it is process and technology.

Redaction & Disclosure: Manual and Unscalable

Missouri's Sunshine Law requires response within three business days regardless of request complexity. A single request for body camera footage from a multi-officer incident may involve recordings from every responding officer, plus dash cam footage, surveillance video, 911 audio, and documents, all requiring review for exempt information under Section 610.021 before release.

Manual redaction of a single 45-minute recording (frame-by-frame blurring, name muting)

can consume hours. At current volumes, this does not scale. The Kansas City Sunshine Law settlement in November 2025 demonstrated how even major agencies fail to meet compliance deadlines. Beyond volume, agencies must now document the legal basis for each redaction decision, a level of rigor manual processes rarely sustain.

> *Core Gap: Manual redaction cannot keep pace with request volume, evidence complexity, or documentation requirements.*

Rethinking the Four Pillars

Addressing these challenges requires a fundamental shift in how each function is approached: from reactive to proactive in surveillance, from fragmented to governed in evidence management, from manual search to intelligent retrieval in investigation, and from labor-intensive to automated in disclosure.

From Reactive to Real-Time Surveillance

Modern surveillance treats live camera infrastructure as an active analytical asset. Video analytics systems operate as a software layer connecting to existing IP cameras via RTSP and ONVIF standards, with no hardware replacement required. They process live feeds continuously, identifying persons, vehicles, weapons, license plates, and suspicious behavior, then routing severity-classified alerts to the right personnel in real time.

Core capabilities include object detection and classification, behavioral analysis such as loitering and

perimeter breach detection, and configurable alerting by severity and confidence level. Custom-trained models support department-specific scenarios, particularly relevant for agencies that face different threat profiles depending on whether they serve urban, suburban, or rural communities.

The result: monitoring staff receive verified, classified alerts with associated video clips instead of watching screens hoping to catch something. Response times improve because officers learn about threats sooner.

> *The Shift: From documenting what happened → to enabling intervention while events are still developing.*

From Fragmented Files to Governed Evidence

Modern evidence management centralizes all digital evidence, regardless of format or source, in a single governed environment with consistent policies and controls. Chain of custody is maintained automatically: every transfer, access, and modification is recorded with user identity, timestamp, and action type. SHA-256 cryptographic hashing verifies that evidence has not been altered since collection. Role-based access controls enforce the FBI CJIS Security Policy's principle of least privilege.

Additional foundational requirements include broad format support across the full range of evidence types agencies encounter, configurable retention policies with legal hold overrides for active litigation, and flexible deployment supporting cloud, on-premises, hybrid, and SaaS models to meet different security postures. For agencies handling CJIS data, the deployment environment must meet FBI CJIS Security Policy requirements. For agencies participating in federal grant programs or sharing evidence across jurisdictions, FedRAMP authorization is increasingly a practical necessity.

Critically, a unified evidence platform creates the foundation the other pillars depend on. Investigation tools need a centralized library to search. Redaction tools need a single system to pull from and return to. Without this backbone, the other capabilities operate in silos.

> *The Shift: From scattered files and manual documentation → to automated, tamper-evident governance from collection to courtroom.*

From Manual Search to Intelligent Investigation

AI-powered investigation tools make large evidence sets searchable without requiring manual review of every file. Visual AI indexes faces, vehicles, weapons, and objects across video and images, making hours of footage searchable in seconds. Instead of scrubbing through a timeline, an investigator can search for a specific vehicle type or clothing description and jump directly to the relevant segments.

Speech-to-text transcription converts audio into searchable, timestamped transcripts with speaker diarization, which is critical for interview analysis and courtroom presentation. AI-generated summaries and chaptering break lengthy recordings into navigable segments with descriptions of what occurs in each, allowing reviewers to understand content without watching end to end.

Conversational AI assistants built on retrieval-augmented generation allow investigators to ask plain-language questions across an entire case and receive answers with direct citations to the exact source and timestamp. Every response is grounded in actual case evidence, not external knowledge, preserving evidentiary integrity. The investigative judgment stays with the detective. The time previously spent searching is redirected to analysis and decision-making.

This also strengthens Brady compliance: when all case evidence is searchable from a single interface, the risk of missing material evidence during disclosure review is significantly reduced.

> *The Shift: From hours of manual footage review → to seconds-fast intelligent retrieval with source citations.*

From Manual Redaction to Automated Disclosure

AI-driven redaction systems identify protected information automatically across video, audio, images, and documents, apply redactions according to predefined policies, and log every decision with the applicable exemption code mapped to legal frameworks such as Missouri Section 610.021 and FOIA exemptions.

Several capabilities separate tools that work at departmental scale from those that do not. Multi-format support matters because a single records request can span video, audio, images, and documents. Bulk processing matters because requests often involve multiple files. Version management matters because different requestors (media organizations, defense attorneys, internal reviewers, and the general public) may each require a different version of the same file. Generating those versions from a single source eliminates duplication of effort.

Automation delivers consistency (the same detection rules apply uniformly across every file), throughput (staff can process significantly more requests without added headcount), and compliance documentation (every redaction is defensibly logged). For Missouri agencies, the ability to handle redaction at speed and scale is directly tied to Sunshine Law compliance, as the three-business-day window leaves no room for manual bottlenecks.

The Shift: From frame-by-frame manual work → to AI-powered redaction with audit-trailed exemption coding at scale.

The Four Pillars in Practice: A Connected Scenario

The greatest value emerges when the pillars work as a connected system. Consider this scenario:

- AI-powered camera analytics detects a weapon near a school and generates a severity-classified alert with the associated video clip.
- The alert and footage are automatically ingested into the evidence management system with full chain of custody from the moment of capture. Responding officers' body-worn camera, dash cam, and 911 audio join the same case.
- A detective searches across all related evidence using AI tools, asks a plain-language question, and receives an answer citing the exact timestamp in the body camera recording.

- When a Sunshine Law request arrives, the redaction tool pulls files from the same platform, applies automated redactions mapped to Section 610.021 exemptions, and returns audit-trailed versions for release within the statutory window.

No thumb drives. No emailed evidence. No broken chain of custody. No days of manual redaction. The technology did not replace anyone's job; it removed the friction that prevented people from doing their jobs effectively.

How VIDIZMO Delivers the Four Pillars Across Public Safety Operations

Rethinking the four pillars requires technology that can operationalize these principles consistently, at scale, and within the security and compliance requirements that law enforcement environments demand. The following solutions address each pillar directly, providing the capabilities that support a modern, connected public safety operation.

VIDIZMO LiveSight Analytics

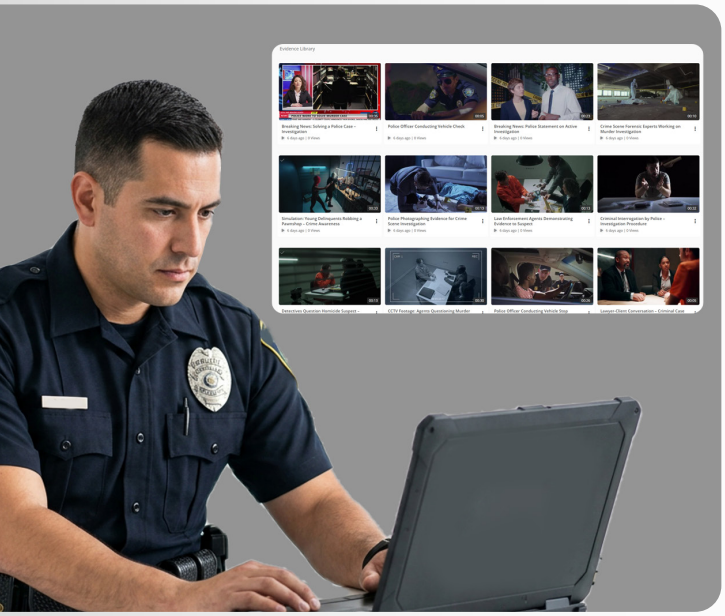
Real-Time Threat Detection on the Infrastructure You Already Have

VIDIZMO LiveSight Analytics delivers real-time AI video analytics on existing camera infrastructure. It operates as a software layer that connects to any IP camera or video management system via RTSP and ONVIF standards, processing up to 32 simultaneous live feeds per server instance and scaling horizontally as camera networks grow.

Pretrained detection models identify persons, faces, weapons, license plates, vehicles, and suspicious activity in real time. Configurable alerts are routed by severity and confidence level to operators, command staff, or integrated systems including email, SMS, and 311 platforms, ensuring the right people are informed at the right time based on predefined detection criteria.

Custom AI models can be trained on agency-specific data for domain-specific detection scenarios. This is particularly relevant for agencies that face different threat profiles depending on whether they serve urban,

suburban, or rural communities. A system that only offers generic detection models will not address the specific scenarios that matter to a given department. No new camera hardware is required.



Digital Evidence Management System

A Single Source of Truth From Collection to Courtroom

VIDIZMO DEMS is a CJIS-compliant, AI-powered digital evidence management system that provides law enforcement agencies with a single governed environment for all digital evidence. It supports ingestion from 255-plus formats including body-worn cameras, dashboard cameras, surveillance footage, 911 audio, interview recordings, photographs, and documents.

Chain of custody is maintained automatically with SHA-256 tamper detection and a complete audit trail of every access and transfer event. Role-based access controls, legal hold capabilities, and configurable retention policies support compliance with FBI CJIS Security Policy requirements. Retention schedules are enforced automatically by case status, evidence type, or jurisdiction, with legal hold overrides for active litigation.

Evidence can be shared securely with prosecutors, defense counsel, courts, and partner agencies through controlled access portals with time-limited, auditable sharing links. Deployment options include SaaS, cloud, on-premises, private cloud, and hybrid environments, allowing agencies to meet their specific security posture and infrastructure requirements.

VIDIZMO Intelligence Hub

From Weeks of Manual Review to Seconds of Intelligent Retrieval

VIDIZMO Intelligence Hub is a multi-modal AI processing platform that transforms how investigators access and interpret case evidence. Its CaseBot capability uses retrieval-augmented generation to allow detectives and analysts to ask plain-language questions across an entire case, including video transcripts, detected objects, document content, and metadata, and receive answers in

seconds with direct citations to the exact source and timestamp.

Automatic transcription in 82 languages with speaker diarization distinguishes between different speakers in a conversation, which is critical for interview analysis and courtroom presentation. AI-generated summarization and automatic chaptering break lengthy recordings into logical segments with descriptions of what occurs in each, allowing reviewers to understand content without watching end to end and then drill into specific segments that require detailed attention.

Intelligence Hub supports deployment on private cloud, on-premises, or air-gapped environments for agencies with strict data residency requirements, and integrates natively with VIDIZMO DEMS. Every AI-generated result is grounded in actual case evidence and traceable to its source, maintaining evidentiary integrity throughout the investigative process.

VIDIZMO Redactor

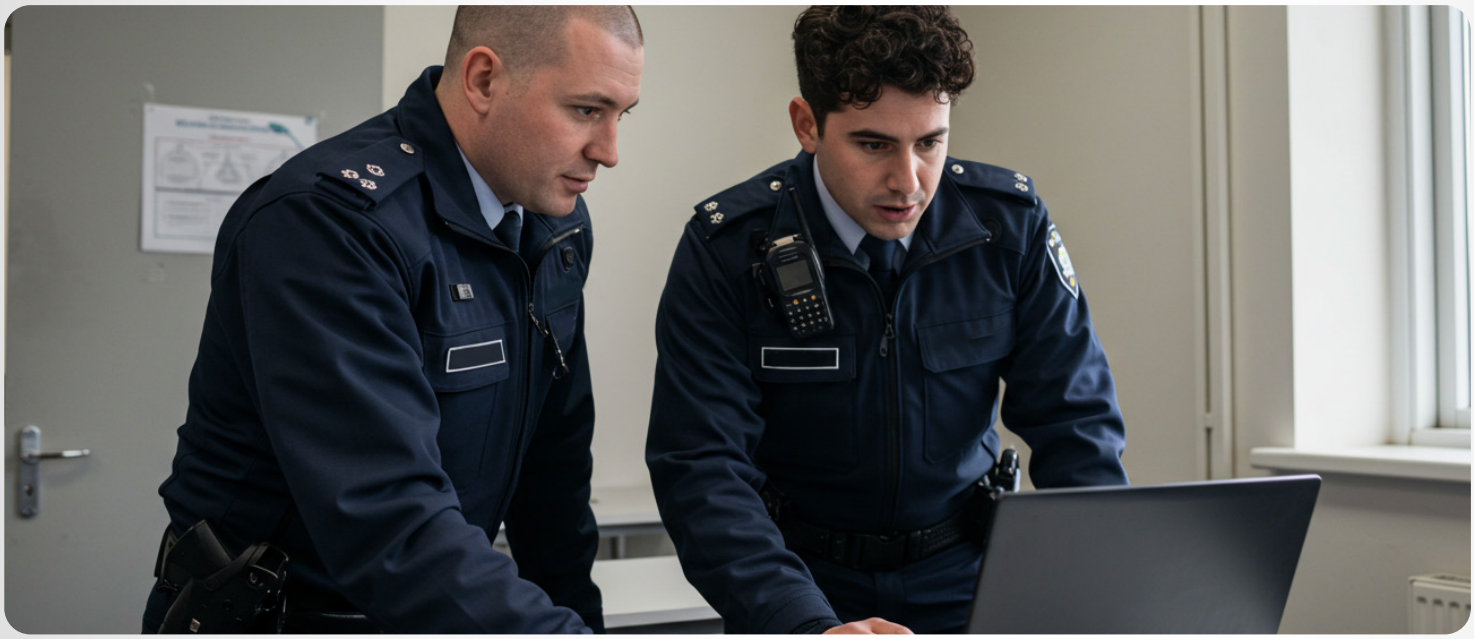
Automated Redaction That Scales With Your Obligations

VIDIZMO Redactor is an AI-powered redaction system that automates the identification and removal of sensitive information across video, audio, images, and documents. It detects and redacts more than 40 categories of personally identifiable information including faces, license plates, and 33-plus categories of spoken PII such as names, addresses, Social Security numbers, and financial identifiers.

Document redaction supports PDF, DOCX, XLSX, PPTX, and scanned documents including handwritten materials, with OCR-based detection and the ability to redact objects embedded as images within PDF files. Every redaction decision is logged with an exemption code mapped to applicable legal frameworks including Missouri Sunshine Law categories under Section 610.021 and FOIA exemptions one through nine, creating a defensible audit trail for every release.

Bulk processing has been tested at scale exceeding one million recordings. Version management allows agencies to generate differently redacted versions of the same file for different audiences (media organizations, defense attorneys, internal reviewers, and the general public) from a single source, eliminating duplication of effort. A managed redaction service with dual quality assurance review is available for agencies that require additional support.

Security and Compliance Across the Platform



Trust in law enforcement operations is built on the consistent, defensible handling of information at every stage. VIDIZMO's platform is engineered to meet these requirements across every deployment model.

CJIS Compliance

All VIDIZMO solutions are built and operated in accordance with FBI CJIS Security Policy standards, covering access control, audit logging, encryption, personnel screening, and incident response across every deployment model.

FedRAMP High Authorization

VIDIZMO supports FedRAMP High deployments through ProjectHost's FedRAMP-authorized environment on Azure Government Cloud. This enables eligibility across federal, state, and local programs and supports federal grant funding for technology procurement.

Encryption & Integrity Verification

AES-256 encryption protects evidence at rest and in transit. SHA-256 cryptographic hashing confirms evidence has not been altered since collection, supporting defensibility in legal proceedings and chain of custody integrity.

Role-Based Access & Audit Logging

Granular role-based access controls enforce the principle of least privilege at the case, folder, or file level. Every user action is logged with timestamp, identity, IP address, and action type for full attribution.

Retention, Legal Hold & Disposition

Automated retention policies enforce schedules by jurisdiction, case type, and regulatory requirement. Legal holds prevent accidental deletion during active litigation. Documented disposition executes when obligations are met, ensuring compliance with NARA and applicable state requirements.

The Four Pillars Are Not Optional. They Are Operational

Traditional approaches built on reactive surveillance, fragmented evidence handling, manual investigation review, and labor-intensive redaction were adequate for an era of lower volumes and less rigorous transparency demands. That era has passed.

When the four pillars are managed as a connected workflow, the benefits compound. Investigations advance in hours instead of days. Automated chain of custody, integrity verification, and documented redaction decisions eliminate the documentation gaps that create legal exposure. Staff time previously consumed by manual review, evidence transfer, and frame-by-frame redaction is returned to active policing, investigation, and case work. Consistent, transparent handling of evidence and public records strengthens institutional credibility in the communities agencies serve.

The factors driving current evidence volumes (body-worn camera mandates, expanded surveillance infrastructure, public records demand) are not temporary. They represent a structural shift. Agencies that build their operational infrastructure around the four pillars today establish a foundation that scales as volumes grow, rather than one that requires repeated reactive adjustment.

From the moment a camera detects a threat to the moment a public records request is fulfilled, the way agencies manage their four operational pillars determines the quality of justice they deliver. By rethinking these pillars today, law enforcement leaders can transform operational burden into strategic advantage.

VIDIZMO.AI

VIDIZMO: The AI-Powered Public Safety Platform

VIDIZMO provides AI-powered solutions purpose-built for law enforcement and public safety. Recognized by Gartner and IDC, the platform spans real-time surveillance analytics, CJIS-compliant evidence management, intelligent case investigation, and automated redaction with full audit trails.

Flexible deployment options (SaaS, cloud, on-premises, hybrid) meet the security posture requirements of agencies at every level of government.

Contact Us

+1 571-969-2180 | sales@vidizmo.ai | www.vidizmo.ai

1775 Tysons Blvd, 5th Floor, Tysons, VA 22102, United States

Follow Us On